Stewart R. Pollock (SBN 301356)
spollock@edelson.com
EDELSON PC
123 Townsend Street,
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Counsel for Plaintiff and the Putative Class

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN FRANCISCO DIVISION

LATISHA SATCHELL, individually and on behalf of all others similarly situated,

Plaintiff,

v.

SIGNAL360, INC., a Delaware Corporation, YINZCAM, INC., a Pennsylvania Corporation, and GOLDEN STATE WARRIORS, LLC, a California Limited Liability Company,

Defendants.

Case No. 16-cv-04961-JSW

CLASS ACTION COMPLAINT FOR:

(1) Violations of the Electronic Communications Privacy Act 18 U.S.C. §§ 2510, *et seq.*

DEMAND FOR JURY TRIAL

FIRST AMENDED CLASS ACTION COMPLAINT

Plaintiff LaTisha Satchell ("Plaintiff or "Satchell") brings this First Amended Class Action Complaint ("Complaint") against Defendants Signal360, Inc. ("Signal360"), Yinzcam, Inc. ("Yinzcam"), and Golden State Warriors, LLC ("Golden State") (collectively "Defendants") based on their unlawful practice of systemically and surreptitiously intercepting consumers' oral communications without their consent. Plaintiff, for her Complaint, alleges as follows upon personal knowledge as to herself and her own acts and experiences and, as to all other matters, upon information and belief, including investigation conducted by her attorneys.

NATURE OF THE ACTION

1. Golden State is one of the premier sports and entertainment organizations in the National Basketball Association ("NBA"), combining its success on the court with its desire to be at

the forefront of technology and fan entertainment off the court.

2. In 2012, Golden State joined the chorus of sports teams in offering a mobile application for its fans. The Golden State Warriors App (the "App" or "Warriors App"), like the team, grew in popularity, with tens of thousands of fans downloading the App and installing it on their smartphones and mobile devices. The App provided an interactive experience for fans by delivering scores, news, and other information relevant to the organization. And, for Golden State, the App is a key source of marketing revenue.

3. Then, in 2014, Defendant Golden State and Signal360 entered into a partnership to establish Golden State as a technological leader among NBA organizations by integrating Signal360's novel beacon technology into the App.

4. This integration was effectuated by Defendant Yinzcam, an app developer, and promised to utilize "beacons" as a method to track consumers and how they interact with marketing and advertisements. With beacons, for instance, advertisers might be able to discern when a consumer is looking at a specific billboard or walking by a concession stand—something previously unprecedented. And with Signal360's integration, Golden State was able to use the App to target specific consumers and send them tailored content, promotions, or advertisements based on their precise location.

5. Defendants' plan to implement beacon technology required two pieces of technology. First, Defendants Golden State and Signal360 worked together to canvas the home stadium of the Warriors (Oracle Area) and other locations (such as retail shops outside of the stadium) with 2-inch by 2-inch beacons that would emit unique audio identifiers.

6. Second, for the beacon technology to work, all Defendants understood that Signal360's technology required active microphones belonging to consumers (i.e., those found on their smartphones, tablets, and other mobile devices) to listen for and hear the unique identifiers emitted by the 2-inch by 2-inch beacons.

7. To facilitate this, Signal360 designed its software to (i) record *all* audio at *all* times—which would necessarily include users' private conversations—and then (ii) analyze

that recorded audio for beacon tones. In this way, Signal360's software functions just like a "bug" designed for mobile devices: Signal360's discrete block of source code turned on users' mobile devices' microphones, constantly recorded audio (including conversations), and analyzed the recorded audio per the Defendants' instructions (references to Signal360's discrete and embedded block of source code is referenced herein as the "Bug"). Thus, Signal360 distributed its software to its partners (here, including Golden State) knowing that its integration and use would necessarily record consumers' conversations.

8. Golden State, in turn, understood that releasing its App with the Bug installed would—when used on consumers' smartphones—cause all audio (including conversations) to be constantly monitored and recorded. By directing Yinzcam to integrate the Bug into the App and then releasing the "bugged" version of the App to the public, Golden State effectively made the decision to "plant" the Bug on hundreds of thousands of mobile devices.

9. In sum, Golden State, Yinzcam (as the App's developer), and Signal360 all understood that once Signal360's software was integrated into the Warriors App, the App would constantly record all audio detectable by its users' mobile devices, which would include users' daily interactions and conversations with others, both in public and private spaces. Nevertheless, Defendants put profits before privacy, and decided to integrate the beacon technology software into the Warriors App.

10. As a result, Defendants gained access to tens of thousands of microphones belonging to consumers who downloaded the Warriors App and turned their mobile devices into bugged listening devices. The App (until recently) did what it was programmed to do: the Bug operating in the Warriors App ventured to ascertain a consumer's precise location by listening to all nearby audio for Signal 360 beacons by secretly activating a consumer's smartphone's built-in microphone. With the Bug activated, it continuously listened to and recorded *all* audio within range—including consumer conversations. If the Bug "heard" one of Signal360's beacons it may have caused the App to display an ad to the consumer or it may have caused the Warriors App to send that information to Defendants Signal360 and Golden State (through the Signal360 content management system).

11. Unfortunately for consumers, Defendants never informed them that their smartphones were being loaded with the Bug (and, thus, would act as a listening device) nor did they ever seek consent. Accordingly, this putative class action seeks (1) to prevent Defendants' nonconsensual listening and recording of consumer conversations, and (ii) statutory and punitive damages for violations under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.* (the "ECPA").

PARTIES

12. Plaintiff LaTisha Satchell is a natural person and resident and citizen of the State of New York.

13. Defendant Sonic Notify, Inc. d/b/a Signal360 is a corporation existing under the laws of Delaware, with its headquarters and principal place of business located at 419 Park Ave., 7th Floor, New York City, New York, 10016. Signal360 conducts business throughout this District, the State of California, and the United States.

14. Defendant Yinzcam, Inc. is a corporation existing under the laws of Pennsylvania, with its headquarters and principal place of business located at 6616 Beacon Street, Pittsburgh, Pennsylvania, 15217. Yinzcam conducts business throughout this District, the State of California, and the United States.

15. Defendant Golden State Warriors, LLC is a limited liability company existing under the laws of California, with its headquarters and principal place of business located at 1011 Broadway, Oakland, California, 94607. Golden State conducts business throughout this District, the State of California, and the United States and is registered to do business in this State (entity number 200420110060).

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction under 28 U.S.C. § 1331 because this action arises under the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510 *et seq.*, a federal statute.

17. This Court has personal jurisdiction over Defendant Signal360 because it conducts

business in California and because the unlawful events giving rise to this lawsuit occurred, in part, in California.

18. This Court has personal jurisdiction over Defendant Yinzcam because it conducts business in California and because the unlawful events giving rise to this lawsuit occurred, in part, in California.

19. This Court has personal jurisdiction over Defendant Golden State Warriors, LLC because it is headquartered in this District, conducts significant business in California, and because the unlawful events giving rise to this lawsuit occurred, in part, in California.

20. Venue is proper in this District under 28 U.S.C. § 1391(b) because a substantial part of the events giving rise to Plaintiff's claims occurred in, were directed to, and/or emanated from this District. 28 U.S.C. § 1391(b).

INTRADISTRICT ASSIGNMENT

21. Pursuant to Civil Local Rule 3-2(d), this case has been assigned to the San Francisco Division.

FACTUAL BACKGROUND

I. An Introduction to Beacon Surveillance Technology.

22. As introduced above, "beacons" are new technologies that seek to track and monitor consumers and how they interact with advertisements and marketing.[2] Fundamental to beacon technology is the smartphone, which consumers carry on their person everywhere they go. And, built into these smartphones are a plethora of radio transmitting and receiving devices, including a "Bluetooth" radio.

23. Bluetooth is a wireless personal area network technology used for transmitting data over short distances. A smartphone with Bluetooth will invariably attempt to communicate with other Bluetooth devices in its vicinity. While those other Bluetooth devices take the form of hands-free car radios, headphones, or stereos, marketers found a new use−canvasing Bluetooth devices in

[2] *Beacon Technology: The Where, What, Who, How and Why*, http://www.forbes.com/sites/homaycotte/2015/09/01/beacon-technology-the-what-who-how-why-and-where/#668c740b4fc1 (last visited March 13, 2017).

specific locations (e.g., retail stores) that exist only to capture an attempted Bluetooth connection. By monitoring which Bluetooth radio (and the corresponding smartphone and owner) attempts to connect to the placed-Bluetooth devices, marketers can track the physical path a smartphone takes through that location.

24. For instance, suppose a department store placed a Bluetooth beacon in its Men's shoes, accessories, and kids departments. A consumer's smartphone, while the consumer navigates from the Men's shoes department to the kids department, would inevitably attempt to connect to the beacon in the Men's shoes and then the kids departments. The retailer now would have a record of that path, which may inform the retailer on certain consumer behavior.

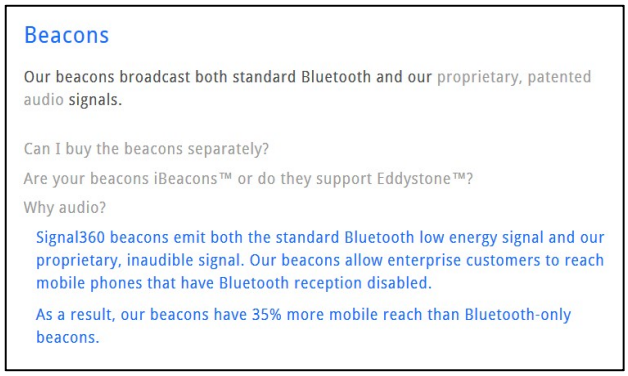
25. The next logical step for marketers was to create beacons that interact more fully with consumers' smartphones. In that same example described above, the retailer might want to cause the consumer's smartphone to "pop up" an alert whenever he or she enters the kids department. The pop up could be a simple text advertising a sale or even a coupon. For this to work, however, the retailer would need access to the consumer's smartphone through an application or a system-wide protocol.

26. Because beacon tracking is inherently invasive (consumers are continuously tracked), industry standards dictate that consumers opt-in to beacon tracking.[3] Often, the form of the opt-in is through the Apple iBeacon protocol in Apple iPhones, or through an application developer's mobile application. If the retailer in the example above operates its own mobile application, it might seek consent through an explicit disclosure or, at least, a privacy policy.

27. Defendant Signal360 utilizes Bluetooth beacons and a novel beacon technology called audio beacons. *See* Figure 1, on the following page. Defendants' audio-based beacon technology, in contrast to Bluetooth beacon technology, requires Defendants to ascertain a consumer's physical location through sounds rather than through radio signals. Instead of canvassing a location with only Bluetooth devices, Signal360 places speakers throughout locations. Each speaker is mapped to a location and emits a unique audio signal. A device that can "hear" a

[3] *Id*.

Signal360 audio beacon must be near that speaker. As such, Signal360 is able to quickly ascertain the location of that device and its approximate distance from the speaker.



(**Figure 1**.)

28. But for the technology to work, Signal360 requires a microphone to continuously listen for its audio signals. For that, Signal360 partnered with Defendants Golden State and Yinzcam and, together, enlisted thousands of sports fans who unwittingly downloaded and installed a "bugged" version of a mobile application from their favorite team.

II. Defendants Partner To Include Audio Beacons in the Warriors' App.

29. Like most sports teams, the Golden State Warriors created an App for its fans to download for free from the Google Play Store (the "Play Store"). To date, the App has been downloaded between 100,000 and 500,000 times.[4] Defendants Golden State and Yinzcam market the App, stating:

> This is the official mobile app of the Golden State Warriors. It delivers an unrivaled interactive team experience by providing the most up-to-date scores, schedules, news, stats, highlights, and photos. The Golden State Warriors app is the easiest way to keep up with everything Warriors basketball. Enhanced with arena information and other amenity features, the Golden State Warriors app is your ultimate game night companion.[5]

30. Among the specific features the App advertises is the ability for consumers to "View live stats, scores and standings" and to "Use #DubNation to share [their] game experience by uploading photos and videos to Facebook, Twitter, Instagram, Pinterest, Google+, Tumblr and

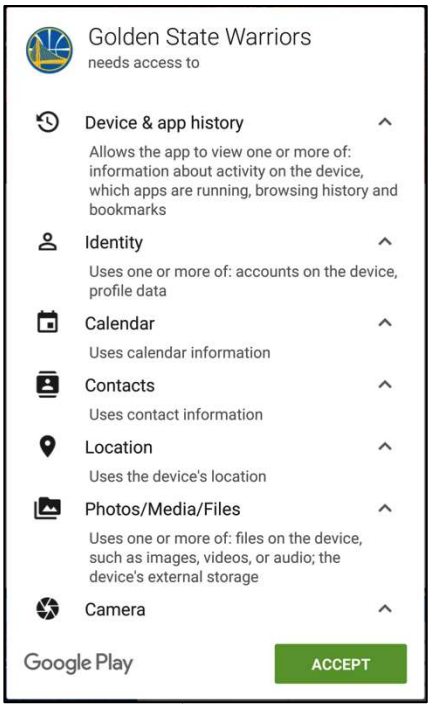
---

[4] *Golden State Warriors - Android Apps on Google Play*, http://web.archive.org/web/20160122133224/https://play.google.com/store/apps/details?id=com.yinzcam.nba.warriors&hl=en (last visited Mar. 13, 2017).

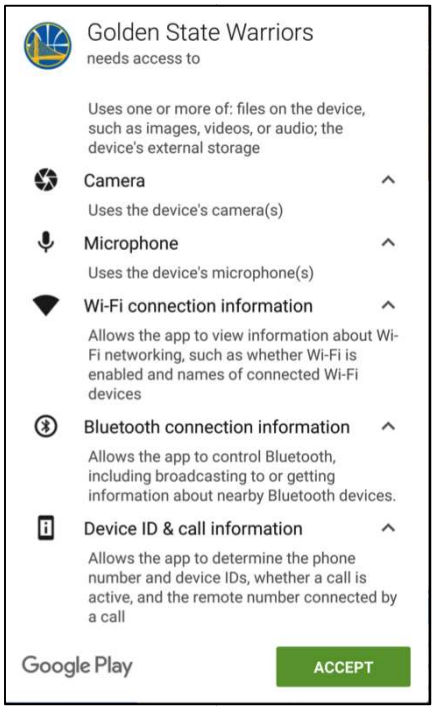
[5] *Id.*

more."

31. Just as with any other application for download in the Play Store, the App asked for certain "permissions." Defendant Yinzcam programmed the App to ask for the following permissions:



(**Figure 2.**)



(**Figure 3.**)

32. Notably absent from the permission list was a request to "opt-in" to the beacon technology—Bluetooth or audio. While the permissions include "microphone," Defendants did not provide any context or information regarding the "microphone." Indeed, a reasonable consumer would view the permission, which is requested right after "Camera," as relating to videos, one of the primary advertised features of the App.

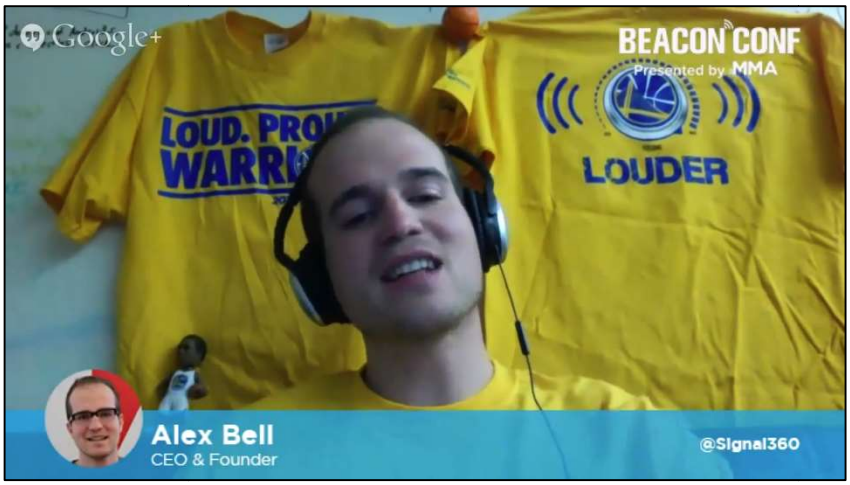
33. Unbeknownst to consumers, though, Defendant Golden State began partnering with Defendant Signal360 (then known as Sonic Notify) in 2014 to "integrat[e] proximity technology into the team's mobile application."[6] Kevin Cote, then senior director of digital for Defendant

[6] *Golden State Warriors enhance game day with beacon technology - Mobile Commerce Daily - Software and technology*, http://web.archive.org/web/20140901104157/http://www.mobilecommercedaily.com/golden-state-warriors-enhance-game-day-with-beacon-technology (last visited Mar. 13, 2017).

Golden State, stated the following about this partnership:

> It's really about using technology to enhance the fan experience … We're not in denial that our fans are going to use their phones during games.
>
> For us it's, "why not enhance their experience to give them special offers or exclusive content[,] informative alerts[,] and more[.]" … Why not integrate it into our mobile app so that the app itself becomes a companion to fans' game day experience.
>
> We were all in with beacon technology. We think it's something that's going to continue to grow, and we're excited to be one of the first sports venues to have full-scale implementation.[7]

34. Indeed, because Defendant Golden State was one of the first to partner with Signal360 to integrate and use its beacon technology, the rollout necessitated complete cooperation between the partners. For instance, in a joint presentation for "BeaconConf" Alex Bell, the CEO and founder Signal360, and Kevin Cote, discussed their joint venture.



(**Figure 4**, showing Signal360 CEO & Founder, Alex Bell, wearing Warriors garb in a joint presentation with Defendant Golden State for "BeaconConf.")

35. In the joint presentation, Golden State's Mr. Cote explained how Golden State and Signal360 worked together to begin a trial run with Signal360's beacon technology that let them "look back on the successes, on the failures, on the education of the fans, on the education our own employees, and the education for us, and for Signal360, too. It was all a learning experience. [N]ow

---

[7] *Golden State Warriors enhance game day with beacon technology - Mobile Commerce Daily - Software and technology*, Mobile Commerce Daily, Mar. 24, 2014, *http://web.archive.org/web/20160408002756/http://www.mobilecommercedaily.com/golden-state-warriors-enhance-game-day-with-beacon-technology* (last visited Mar. 13, 2017).

... the technology has improved, options have improved, and that's really made it[.] [I]nternally here the light bulbs have gone off and we have been able to prove how to help drive the business, most importantly."

36. In Golden State, Signal360 found a partner willing to use its fan base as a test bed for unproven and intrusive tracking technology. In another presentation, Alex Bell seemingly acknowledged as much:

> [Signal360's beacon technology] only ever works when someone in the organization says "I'm going to be that champion, and I'm going to grab ahold of this," like the Golden State Warriors. And it's up to them to find a partner like us who is going to make them a champion because it's going to be easy.

37. Worse, Signal360 and Golden State both knew and understood that Warriors fans would implicitly trust the Warriors and install a seemingly innocuous app onto their smartphones. According to a Bloomberg article, fan loyalty created the conditions ripe for "experimentation":

> Sonic Notify, the company that installed several dozen 2-by-2-inch beacons in Oracle Arena, says sports franchises are the ideal businesses to use this kind of technology. Stores have to worry about annoying their shoppers, says Aaron Mittman, the company's chief executive officer, while sports fans are more open to experimenting. "*You're not going to get mad at the Golden State Warriors and go to some other arena instead*," he says.[8]

38. This exploitation of fan trust seemingly paid off. According to a fact sheet, the partnership between Golden State and Signal360 has been "astounding" because they "worked together to drive incremental seat upgrade revenue." *See* Figure 5:

* * * *

[8] *Sonic Notify Uses Phones to Bug Fans Who Buy Cheap Seats*, https://www.bloomberg.com/news/articles/2014-03-20/sonic-notify-uses-phones-to-bug-fans-who-buy-cheap-seats (last visited Mar. 13, 2017).

(**Figure 5.**)

39. But while Defendants profited, consumers were left in the dark on how the Warriors App operated. The App's Terms of Service, Privacy Policy, and system settings' entries were silent as to the App's use of beacons.[9] At no time did Defendants disclose to consumers that the Warriors App used beacon technology. And—more to the point—Defendants did not disclose that the Warriors App used audio beacon technology that surreptitiously turned on consumers' smartphone microphones and, thereafter, recorded all surrounding audio (including users' conversations).

III. Defendants Hijacked Users Smartphones And Turned Them Into Listening Devices.

40. A forensic accounting of the Warriors App revealed exactly how the App operated and uncovered Defendants' ability to remotely eavesdrop on consumers' lives through the Bug.

41. Upon startup, Defendants never sought permission, either through the Warriors App or through the Bug, to begin listening in. Instead, Defendant Yinzcam, at the direction of Defendants Golden State and Signal360, programmed the Warriors App to instantly initiate the Bug once the App was installed and opened. The Bug then executed commands programmed by Defendant Signal360 to communicate with Signal360's servers. The Signal360 servers would then respond with a command to turn on the Bug, which was programmed at the request of Defendant

[9] *Mobile App Privacy Policy*, http://www.yinzcam.com/?page_id=234 (last visited Mar. 13, 2017).

Golden State. Specifically, Defendant Golden State worked with Defendant Signal360 to specifically identify rules and terms for their beacon scheme and knew that those rules and terms would be transmitted to the tens of thousands of devices and, in turn, would cause the Bugs on those devices to activate and, thus, turn users' smartphones into listening devices.

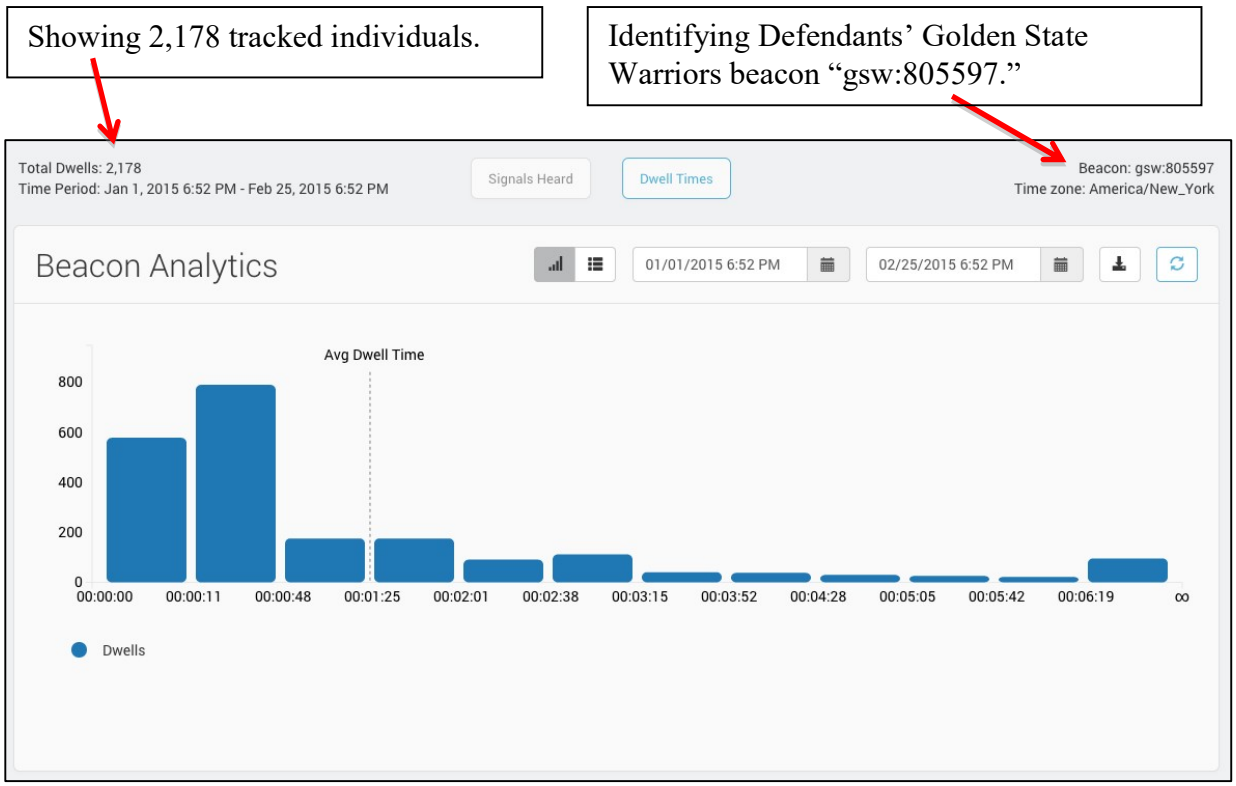
42. That is, once consumers downloaded and opened the Warriors App, the App would engage the Bug, receive an OK from Signal360's server (per the rules created by Golden State), and turn on consumers' microphones, listening and picking up any and all audio within range of a user's microphone. The Bug continued listening until its process was closed—either when the consumer's smartphone was shut off or when the consumer manually stopped the Bug's process (something consumers ignorant of the Bug would not know to do). By design, the Bug listened even when the Warriors App was running in the background, such as when a consumer used the Warriors App but then pressed the home button, switches to another app, or shuts off the smartphone's screen.

43. When it was listening (effectively all the time), the Bug temporarily recorded audio and retained portions of the audio for further analysis. Defendants programmed the Bug to analyze and monitor the picked-up audio for any of the Signal360 beacon tones. For instance, if the Bug heard a transmitter's audio signal in its recordings, the Bug would cause the Warriors App to automatically respond by, for instance, displaying banner advertisements to the consumer or by chronicling consumer location for later analysis.

44. To be most effective, Defendants' Bug, was designed to use users' microphones at all times while the Warriors App was installed and the Bug process was running on a smartphone. This allowed Defendants' audio-based marketing tool to determine when a consumer was within range of an audio-based beacon transmitter and when they were not. Regardless of whether it was being actively used or running in the background, consumers were kept ignorant of the App's (and the Bug's) listening capabilities.

45. To monitor the effectiveness of Defendants' beacon scheme, Defendants Signal360 and Golden State both had access to data generated by the Bug and the Warriors App. Figure 6 is a screenshot from the Signal360 analytics platform called the Signal360 content management system

("CMS"). With the CMS, Defendants could "track a number of different metrics by date and time range, and by single or groups of content-type, beacon, and location. Tracked metrics include: number of beacon signals heard by mobile users, number of user engagements with delivered content, and amount of time the mobile user is in physical proximity of a particular beacon. In addition, in-location customer path and group data is available."



(**Figure 6,** showing Defendants' surreptitious monitoring of 2,178 individuals and how long each "dwells" at a particular location.)

FACTS RELATED TO PLAINTIFF LATISHA SATCHELL

46. Plaintiff LaTisha Satchell downloaded the App in or around April, 2016. As soon as the App downloaded, Plaintiff opened the App. Plaintiff continued to use the App to follow the progress of the Golden State Warriors. Plaintiff paid close attention to the Golden State Warriors at this time and used the App at least once per day because the team competed in the 2016 NBA playoffs and reached the 2016 NBA Finals. Plaintiff stopped using the App and attempted to disable the Bug on or about July 11, 2016.

47. From April 2016 until July 11, 2016, Plaintiff carried her smartphone on her person. She would take her smartphone to places where she would not invite other people, and to places

where she would have private conversations. That is, her phone was present in locations and personal and private situations not generally accessible to the public where the expectation was that her conversations were to remain private. During this entire time, the Bug's process was running.

48. Unbeknownst to Plaintiff and without her consent, Defendants programmed the App to include the Bug that, once activated, turned on her smartphone's microphone and thereby caused the App to constantly record all audio, including conversations. Specifically, because Plaintiff carried her smartphone to locations where she would have private conversations and the Bug was continuously running on her phone, the Bug listened-in to private oral communications.

49. For instance, Plaintiff engaged in many private conversations during this time period, where she carried her phone (with the Bug running) on her person, and, therefore, had those conversations recorded by Defendants. Examples of those conversations included, among many others:

- On April 21, 2016, Plaintiff was in her bedroom with her husband, had her phone with her, and engaged in nightly marital conversations;
- On May 12, 2016, Plaintiff was in a conference room with approximately 50 other people for a business meeting, had her phone with her, and discussed non-public information;
- On June 28, 2016, Plaintiff was at a local real estate office meeting with a loan officer, had her phone with her, and discussed private financial matters;
- On July 1, 2016, Plaintiff was at a local bank meeting with a banker, had her phone with her, and discussed private financial matters.

50. In each of the instances described above, Plaintiff believed that she was conversing in private and would not have engaged in the specific conversations had she known that the App (via the Bug) was recording her conversations. Despite her expectations of privacy, however, the "bugged" version of the App was recording her conversations.

51. At no time did Plaintiff consent to the App or the Bug using her microphone to continuously listen-in to her oral conversations. While Plaintiff was using the App (i.e., from April 2016 until July 11, 2016), Plaintiff was unaware of the Bug and did not ever close or stop the Bug process.

CLASS ALLEGATIONS

52. **Class Definition**: Plaintiff brings this action pursuant to Fed. R. Civ. P. 23(b)(2) and (3) on behalf of herself and a Class of similarly situated individuals, defined as follows:

> All individuals in the United States who downloaded and opened the Golden State Warriors mobile application that included but did not disclose the presence of Signal360 audio beacon code.

Excluded from the Class is: (1) any Judge or Magistrate presiding over this action and members of their families; (2) Defendants, Defendants' subsidiaries, parents, successors, predecessors, and any entity in which the Defendants or their parents have a controlling interest and their current, former, purported, and alleged employees, officers, and directors; (3) counsel for Plaintiff and Defendants; (4) persons who properly execute and file a timely request for exclusion from the Class; (5) the legal representatives, successors, or assigns of any such excluded persons; and (6) all persons who have previously had claims similar to those alleged herein finally adjudicated or who have released their claims against Defendants.

53. **Numerosity**: The exact number of Class members is unknown to Plaintiff at this time, but it is clear that individual joinder is impracticable. Defendants have listened in on thousands of consumers who fall into the Class definition. Ultimately, the Class members will be easily identified through Defendants' records.

54. **Commonality and Predominance**: There are many questions of law and fact common to the claims of Plaintiff and the Class, and those questions predominate over any questions that may affect individual Class members. Common questions for the Class include, but are not necessarily limited to the following:

a) whether Defendants listened to and/or recorded the Class members' oral communications;

b) whether Defendants obtained consent to listen to and/or record the Class members' oral communications;

c) whether Defendants' conduct violates the Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*; and

d) whether Plaintiff and the Class members are entitled to equitable relief as well as actual and/or statutory damages resulting from Defendants' conduct.

55. **Typicality**: Plaintiff's claims are typical of the claims of all the other Class members. Plaintiff and the Class members sustained substantially similar damages as a result of Defendants' uniform wrongful conduct, based upon the same interactions that were made uniformly with Plaintiff and the public.

56. **Adequate Representation**: Plaintiff will fairly and adequately represent and protect the interests of the other Class members. Plaintiff has retained counsel with substantial experience in prosecuting complex litigation and class actions. Plaintiff and her counsel are committed to vigorously prosecuting this action on behalf of the Class members and have the financial resources to do so. Neither Plaintiff nor her counsel has any interest adverse to those of the other Class members.

57. **Policies Generally Applicable to the Class**: Defendants have acted and failed to act on grounds generally applicable to Plaintiff and the other Class members, requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward the Class.

58. **Superiority**: This case is also appropriate for class certification because class proceedings are superior to all other available methods for the fair and efficient adjudication of this controversy as joinder of all parties is impracticable. The damages suffered by individual Class members will likely be relatively small, especially given the burden and expense of individual prosecution of the complex litigation necessitated by Defendants' actions. Thus, it would be virtually impossible for individual Class members to obtain effective relief from Defendants' misconduct. Even if Class members could sustain such individual litigation, it would still not be preferable to a class action, because individual litigation would increase the delay and expense to all parties due to the complex legal and factual controversies presented in this Complaint. By contrast, a class action presents far fewer management difficulties and provides the benefits of single adjudication, economies of scale, and comprehensive supervision by a single Court. Economies of time, effort, and expense will be fostered and uniformity of decisions ensured.

59. Plaintiff reserves the right to revise the Class Definitions and Class Allegations based on further investigation, including facts learned in discovery.

FIRST CAUSE OF ACTION
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1)(a)
Against All Defendants
(On Behalf of Plaintiff and the Class)

60. Plaintiff incorporates by reference the foregoing allegations.

61. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.* prohibits any person from intentionally intercepting any oral communication or from intentionally using, or endeavoring to use, the contents of any oral communication while knowing or having reason to know that the information was obtained through the interception of an oral communication. 18 U.S.C. §§ 2511(1)(a), (d).

62. Plaintiff and each member of the Class downloaded and installed the Golden State App with Defendant Signal360's audio beacon technology built in.

63. During the time Plaintiff and the members of the Class had (or still have) Defendants' App on their smartphones, Defendants intercepted (by listening in and recording) Plaintiff's and the Class's private conversations, including oral communications, where Plaintiff and the Class exhibited expectations that such communications were to remain private and would not otherwise be subject to interception under circumstances justifying such expectation. 18 U.S.C. § 2510(2).

64. Golden State leveraged its mobile application with a large number of consumers who downloaded and installed the App (likely between 100,000-500,000 individuals) to serve as the host of the Signal360 audio beacon technology. Reasonable consumers that downloaded the App had no way of knowing that the requested "microphone" permission would result in the surreptitious monitoring of their oral communications. Instead, consumers trusted Golden State when they downloaded the application. And when Golden State requested the microphone permission, consumers trusted that it was for some disclosed purpose (e.g., video). Without Golden States' trusting fans, Defendants could not have obtained access to enough microphones for their scheme to be viable.

65. At all times during this scheme, Defendant Golden State distributed the Warriors App knowing that it contained the Bug and, once installed, would constantly record all audio (i.e., it

knowingly turned its users' phones into listening devices). Moreover, Golden State worked with Defendant Signal360 to identify rules and terms for their beacon scheme and knew that its rules and terms would be transmitted to the tens of thousands of devices causing the Bugs on those devices to activate.

66. Defendant Signal360, for its part, not only provided the specific technology at issue here, but was and is integral to the continued operation of the listening device. Specifically, Signal360 owns and controls the Bug's codebase that Yinzcam and Golden State put in the Warriors App that causes consumers' microphones to activate. Moreover, without Signal360's servers communicating with each listening device on each smartphone to send the rules and terms to consumers' smartphones, the Bug would not have been activated. As a result, Signal360's actions are an integral link in the development and operation of the listening device (i.e., the App) that performs the unlawful interceptions at issue.

67. Defendant Yinzcam developed and maintained the codebase of the Warriors App and ensured the deliverability of the App to the Google Play Store and, ultimately, consumers. Specifically, Yinzcam received the Signal360 Bug source code and integrated it into the source code of the Warriors App. Then, Yinzcam conducted testing to ensure that the Bug would cause users' microphones to turn on and begin listening, that the Warriors App would work seamlessly with the Bug, and that the Warriors App would respond appropriately when the Bug heard a Signal360 beacon. Finally, Yinzcam, either using its existing Google Play Developer account or creating a new account, uploaded the source code of the Warriors App containing the Bug to the Google Play Developer Console. Then, it could have conducted "alpha and beta tests" of the Warriors App with the Bug to conduct testing or it could have caused the Warriors App containing the Bug to be published in the Google Play Store, even as the App did not disclose the presence of the Bug. Yinzcam's actions are an integral link in the development and distribution of the listening device (i.e., the App) that performs the unlawful interceptions at issue.

68. Defendants did not inform nor obtain consent from Plaintiff or the Class to listen to and record their private conversations. Plaintiff and the Class had no reason to know or suspect that

the App would constantly and continuously record and analyze their conversations.

69. As detailed herein, once the App is downloaded and opened on their smartphones, Defendants listen to and record oral communications belonging to Plaintiff and members of the Class and use the contents of the captured audio to their economic benefit, including for marketing purposes.

70. At all times, Defendants acted intentionally by programming the App to specifically turn on users' microphones without consent.

71. As a proximate cause of Defendants' violation of the ECPA, Plaintiff and members of the Class have been injured by and through the wear and tear on their smartphones, consuming the battery life of their smartphones, and diminishing their use, enjoyment, and utility of their devices.

72. Plaintiff and the Class members suffered harm as a result of Defendants' violations of the ECPA, and therefore seek (a) preliminary, equitable and declaratory relief as may be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendants as a result of its unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

SECOND CAUSE OF ACTION
Violation of the Electronic Communications Privacy Act
18 U.S.C. § 2511(1)(b)
Against All Defendants
(On Behalf of Plaintiff and the Class)

73. Plaintiff incorporates by reference the foregoing allegations.

74. An entity violates the Electronic Communications Privacy Act, 18 U.S.C. § 2511(1)(b) when it intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication" and one of the following is true:

> (i) such device is affixed to, or otherwise transmits a signal through, a wire, cable, or other like connection used in wire communication; or
>
> (ii) such device transmits communications by radio, or interferes with the transmission of such communication; or

> (iii) such person knows, or has reason to know, that such device or any component thereof has been sent through the mail or transported in interstate or foreign commerce; or
>
> (iv) such use or endeavor to use (A) takes place on the premises of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or (B) obtains or is for the purpose of obtaining information relating to the operations of any business or other commercial establishment the operations of which affect interstate or foreign commerce; or
>
> (v) such person acts in the District of Columbia, the Commonwealth of Puerto Rico, or any territory or possession of the United States[.]

18 U.S.C. §§ 2511(1)(b).

75. The Signal360 Bug is an "electronic, mechanical, or other device" as is defined by 18 U.S.C. § 2510 (5) because it can be used to intercept oral communications.

76. Plaintiff and each member of the Class downloaded and installed an application with Defendant Signal360's audio beacon technology, the Bug, built in.

77. During the time Plaintiff and the members of the Class had the applications with Defendant Signal360's audio beacon technology (the Bug) built in and active, Defendant Signal360 used the Bug to intercept (by listening in and recording) Plaintiff's and the Class's private conversations, including oral communications, where Plaintiff and the Class exhibited expectations that such communications were to remain private and would not otherwise be subject to interception under circumstances justifying such expectation. 18 U.S.C. § 2510(2).

78. And as described throughout, Defendant Yinzcam and Golden State procured Signal360 to implement and use the Bug as a part of the scheme to implement beacon technology (which they knew would necessarily involve the recording of consumers' conversations), and Signal360 used the Bug to intercept Plaintiff's and the Class's oral communications.

79. In the alternative to paragraph 78, Defendant Yinzcam and Golden State procured the Bug from Signal360 as a part of the scheme to implement beacon technology, and Defendants jointly used the Bug to intercept Plaintiff's and the Class's oral communications.

80. Defendants' actions occurred:

a. in violation of 18 U.S.C. 2511(1)(b)(ii) because the Bug was designed to integrate with the App to send information over wireless internet connections

(e.g., "communications by radio");

b. in violation of 18 U.S.C. 2511(1)(b)(iii) because Defendants knew that the Bug device was distributed through the internet by and through the Google Play Store (e.g., transported in interstate commerce);

c. in violation of 18 U.S.C. 2511(1)(b)(iv) because Defendant Signal360 used the Bug device (and specifically designed the Bug for use) on the premises of any business (e.g., the Oracle Arena used for *National* Basketball Association games) and used the Bug for the purpose of obtaining information related to the operations of the Golden State Warriors of the NBA (e.g., by seeking to hear beacon signals); and,

d. in violation of 18 U.S.C. 2511(1)(b)(v) because, on information and belief, Defendants acted in the District of Columbia (e.g., the Bug was designed to operate anywhere in the United States and the App has been downloaded between 100,000 and 500,000 times, likely including by many persons in the District of Columbia).

81. Defendants did not inform nor obtain consent from Plaintiff and the Class to listen in and/or record their private conversations. Plaintiff and the Class had no reason to know or suspect that Defendants would constantly and continuously record and analyze their conversations.

82. As detailed herein, Defendants programmed the App with the Bug device to listen to and record oral communications belonging to Plaintiff and members of the Class as soon as technically feasible and use the contents of the audio captured to its economic benefit, including for marketing purposes.

83. At all times, Defendants acted intentionally by using the Bug device (Signal360) or procuring Signal360 to use the Bug device (Golden State and Yinzcam) without Plaintiff's and Class members' consent.

84. Plaintiff and the members of the Class suffered harm as a result of Defendants' violations of the ECPA, and therefore seek (a) preliminary, equitable and declaratory relief as may

be appropriate, (b) the sum of the actual damages suffered and the profits obtained by Defendants as a result of their unlawful conduct, or statutory damages as authorized by 18 U.S.C. § 2520(2)(B), whichever is greater, (c) punitive damages, and (d) reasonable costs and attorneys' fees.

PRAYER FOR RELIEF

WHEREFORE, Plaintiff LaTisha Satchell, on behalf of herself and the Class, respectfully requests that this Court enter an Order:

A. Certifying this case as a class action on behalf of the Class defined above, appointing Plaintiff LaTisha Satchell as representative of the Class, and appointing her counsel as Class Counsel;

B. Declaring that Defendants' actions, as described herein, violate the Electronic Communications Privacy Act (18 U.S.C. §§ 2510 *et seq.*);

C. Awarding statutory damages in the amount of whichever is the greater of (a) the sum of actual damages suffered plus any profits Defendants earned through its unlawful conduct, or (b) the greater of $100 per Class member, per day of Defendants' violations, or $10,000 per Class member, pursuant to 18 U.S.C. § 2520(c)(2);

D. Awarding punitive damages as appropriate;

E. Awarding injunctive relief as necessary to protect the interests of Plaintiff and the Class members, including, *inter alia*, an order prohibiting Defendants from listening to and recording consumer oral communications in compliance with the ECPA;

F. Awarding Plaintiff and the members of the Class their reasonable litigation expenses and attorneys' fees;

G. Awarding Plaintiff and the members of the Class pre- and post-judgment interest, to the extent allowable; and

H. Awarding such other and further relief as equity and justice may require.

JURY TRIAL

Plaintiff demands a trial by jury for all issues so triable.

Respectfully submitted,

LATISHA SATCHELL, individually and on behalf of all others similarly situated,

Dated: March 13, 2017

By: /s/ Benjamin S. Thomassen
One of Plaintiff's Attorneys

Rafey S. Balabanian*
rbalabanian@edelson.com
Eve-Lynn J. Rapp*
erapp@edelson.com
Stewart R. Pollock (SBN 301356)
spollock@edelson.com
EDELSON PC
123 Townsend Street
San Francisco, California 94107
Tel: 415.212.9300
Fax: 415.373.9435

Benjamin S. Thomassen*
bthomassen@edelson.com
EDELSON PC
350 North LaSalle Street, 13th Floor
Chicago, Illinois 60654
Tel.: (312) 589-6370
Fax.: (312) 589-6378

Counsel for Plaintiff and the Putative Class

**Admitted pro hac vice.*